Section:	06	Title:	Information Security
Sub Section:	01	Title:	General Policy
Document:	07	Title:	Arizona Computer Emergency Response Team (AZCERT)

1. STANDARD

ISD Security will maintain procedures to detect, investigate, and respond to all security incidents.

1.1. Summary of Standard Changes

- Title change to Arizona Computer Emergency Response Team (AZCERT)
- Reference to handbook on AZCERT

1.2. Purpose

To detect and analyze threats to all state assets providing proper responses to minimize harm, loss, and/or liability caused by the associated threats.

1.3. Scope

Applies to all security incidents in the areas of information, physical, communications, and personnel security.

1.4. Responsibilities

1.4.1. Management will support security procedures and recommendations of Arizona Computer Emergency Response Team (AZCERT).

1.4.2. The AZCERT will respond to security incident situations and determine response and corrective measures.

1.4.3. All employees and users of ISD and its systems will report all incidents whether they are perceived as possibilities, or are, or have occurred.

1.5. Definitions and Abbreviations

1.6. Description of Standard

AZCERT will deal with security incidents. Necessary detection devices will be instituted to identify security incidents in the areas of access to information, communications, facilities access, protection of equipment, and misuse of state assets in all areas. Safety and loss control activities will also be monitored. When an incident is perceived, the AZCERT will provide investigation, conduct analysis, and determine responses with recommended corrective measures to block like occurrences in the future as outlined in the AZCERT Handbook.

1.7. Implications

Section:	06	Title:	Information Security
Sub Section:	01	Title:	General Policy
Document:	07	Title:	Arizona Computer Emergency Response Team (AZCERT)

The ISD Security Manager will create procedures to detect security incidents in all areas of concern. The Security Manager will create, and chair, an AZCERT to determine directions for investigation and necessary response and corrective actions for any security incident.

1.8. References

State Standard P800-S855 Incident Response and Reporting

1.9. Attachments

2. SECURITY INCIDENT REPORTING PROCEDURES

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. When a incident is anticipated or detected by any employee, they will immediately report their concerns to the ISD Security Manager, or if unavailable any member of AZCERT. Within two hours, the employee will be re-contacted confirming actions being instituted. If re-contact does not occur, the employee immediately contacts their manager detailing the situation who will provide accelerated problem notification.

2.2.2. The ISD Security Manager acts as the central point of contact for all information concerning security incidents.

2.3. References

2.4. Attachments

3. SECURITY INCIDENT AZCERT PROCEDURES

3.1. Summary of Procedure Changes

3.2. Procedure Details

3.2.1. AZCERT will be appointed by the ISD Security Manager with full management support from management level personnel who posses superior diagnostic and technical problem solving skills. They will have good communications skills and the

ability to resolve technical problems without fueling emotions or adding complications. The members will by able to identify and coordinate department resources necessary to deal with all types of security incidents.

3.2.2. Upon notification of a security incident, the ISD Security Manager will convene AZCERT who will perform a basic risk assessment, determine damage control measures and problem correction procedures, and report recommendations to the ISD Deputy Director or his designee.

3.2.3. At the conclusion of the incident, AZCERT will produce a report documenting all aspects of the incident, how it was handled, and the results of actions taken.

3.3. References

AZCERT Handbook (in draft).

3.4. Attachments